

09/889056

FR00
03230

REC'D 29 JAN 2001

WIPO

PCT

BREVET D'INVENTION

EU

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **08 DEC. 2000**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1 a) OU b)

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
<http://www.inpi.fr>

THIS PAGE BLANK (USPTO)

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 260899

REMISE DES PIÈCES DATE 23 NOV 1999 LIEU 75 INPI PARIS B N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 9914755 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 23 NOV. 1999		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE BULL S.A. Monsieur Jean-Marc DIOU 68, route de Versailles PC : 58D20 78434 LOUVECIENNES Cedex	
Vos références pour ce dossier <i>(facultatif)</i> FR 3876 JMD			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N° _____ Date ____ / ____ / ____ N° _____ Date ____ / ____ / ____	
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N° _____ Date ____ / ____ / ____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Dispositif informatique pour sécuriser des messages au niveau d'une couche réseau.			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date ____ / ____ / ____ Pays ou organisation _____ N° _____ Date ____ / ____ / ____ Pays ou organisation _____ N° _____ Date ____ / ____ / ____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		BULL S.A.	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		6 4 2 0 . 5 8 7 3 9	
Code APE-NAF		3 0 0 . C	
Adresse	Rue	68, route de Versailles	
	Code postal et ville	78430 LOUVECIENNES	
Pays		France	
Nationalité		Française	
N° de téléphone <i>(facultatif)</i>		01.39.66.61.81	
N° de télécopie <i>(facultatif)</i>		01.39.66.71.71	
Adresse électronique <i>(facultatif)</i>		jean-marc diou@bull.net	

Réservé à l'INPI

REMISE DES PIÈCES

DATE

23 NOV 1999

LIEU

75 INPI PARIS B

N° D'ENREGISTREMENT

NATIONAL ATTRIBUÉ PAR L'INPI

9914755

DB 540 W / 260899

Vos références pour ce dossier :
(facultatif)

FR 3876 JMD

6 MANDATAIRE

Nom

DIOU

Prénom

Jean-Marc

Cabinet ou Société

BULL S.A.

N° de pouvoir permanent et/ou
de lien contractuel

PG 4972

Adresse

Rue

68, route de Versailles

Code postal et ville

78430 LOUVECIENNES

N° de téléphone (facultatif)

01.39.66.61.81

N° de télécopie (facultatif)

01.39.66.71.71

Adresse électronique (facultatif)

jean-marc diou@bull.net

7 INVENTEUR (S)

Les inventeurs sont les demandeurs

☐ Oui

☒ Non Dans ce cas fournir une désignation d'inventeur(s) séparée

8 RAPPORT DE RECHERCHE

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat
ou établissement différé

☒

☐

Paiement échelonné de la redevance

Paiement en trois versements, uniquement pour les personnes physiques

☐ Oui

☐ Non

**9 RÉDUCTION DU TAUX
DES REDEVANCES**

Uniquement pour les personnes physiques

☐ Requête pour la première fois pour cette invention (joindre un avis de non-imposition)

☐ Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :

Si vous avez utilisé l'imprimé «Suite»,
indiquez le nombre de pages jointes

**10 SIGNATURE DU DEMANDEUR
OU DU MANDATAIRE**
(Nom et qualité du signataire)

Jean-Marc DIOU (Mandataire Bull S.A)

**VISA DE LA PRÉFECTURE
OU DE L'INPI**

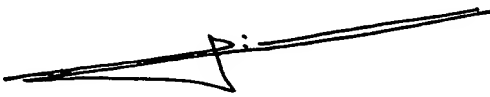
DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° **1/1**
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		FR 3876 JMD	
N° D'ENREGISTREMENT NATIONAL		9514 755	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Dispositif informatique pour sécuriser des messages au niveau d'une couche réseau.			
LE(S) DEMANDEUR(S) :			
BULL S.A. 68, route de Versailles 78430 LOUVECIENNES			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		Cunchon	
Prénoms		François	
Adresse	Rue	5, rue Claude Nicolas Ledoux	
	Code postal et ville	78114 Magny les Hameaux	
Société d'appartenance (facultatif)			
Nom		Martin	
Prénoms		René	
Adresse	Rue	32, rue de Gometz	
	Code postal et ville	91440 Bures sur Yvette	
Société d'appartenance (facultatif)			
Nom		Tran Minh	
Prénoms		Lap	
Adresse	Rue	18, rue Paul Eluard	
	Code postal et ville	95360 Montmagny	
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Louveciennes, le 22 novembre 1999  Jean-Marc DIOU (Mandataire Bull S.A.)	

THIS PAGE BLANK (USPTO)

Dispositif informatique pour sécuriser des messages au niveau d'une couche réseau.

Le domaine de l'invention est celui des réseaux informatiques et plus particulièrement celui de la sécurisation d'acheminement de messages sur ces réseaux.

5

Un réseau public tel que le réseau Internet, permet d'interconnecter de nombreux réseaux privés reliés par des points d'accès et des routeurs qui acheminent les messages. La facilité d'accès à un tel réseau est un avantage pour le libre parcours des idées et de nombreuses connaissances, c'est aussi un inconvénient pour la confidentialité de certaines informations. C'est pourquoi il convient de sécuriser certains messages de façon à ce que seul le destinataire puisse les comprendre, soit assuré de leurs provenances et ou de leur intégrité.

10

Un traitement de sécurisation de messages est envisageable dans différentes couches de communication d'un dispositif informatique. Par exemple, dans une couche utilisateur, une application telle que http, ftp ou mail, peut se charger d'effectuer des traitements de cryptage et décryptage, de signature et d'authentification. Généralement, le message n'est disponible que dans la couche utilisateur de l'émetteur initial et du récepteur final.

15

Selon l'état de la technique, on peut prévoir de faire le traitement de sécurisation dans une couche réseau où une couche de sécurité réseau telle que Ipsec prend en charge le traitement de sécurisation au niveau même du routage des messages. Ceci permet de créer des réseaux privés virtuels qui empruntent les ressources du réseau public au moyen d'un effet tunnel connu. La couche réseau est généralement considérée comme une ressource de communication d'un dispositif informatique. La mise en œuvre de la couche de sécurité réseau qui résulte de cette considération, dans la couche noyau d'un système d'exploitation du dispositif informatique, décharge alors la couche utilisateur des traitements de sécurisation.

25

Cependant, certains traitements de sécurisation sont longs car ils appliquent de nombreux calculs sur le contenu d'un message à sécuriser. Une attente du système d'exploitation sur un retour de fonction qui donne le résultat de traitement présente l'inconvénient de bloquer le dispositif informatique.

30

L'objet de l'invention est un dispositif informatique comprenant une mémoire et une couche de sécurité réseau pour appliquer un traitement de sécurisation sur présentation d'un message dans la mémoire. Pour pallier l'inconvénient précédemment cité, le dispositif informatique est caractérisé en ce que:

- 5 - la présentation du message fait passer la couche de sécurité réseau d'un état initial à un premier état qui réalise une sauvegarde de contexte d'exécution dans une zone de la mémoire;
- la réalisation de la sauvegarde du contexte d'exécution, fait passer la couche de sécurité réseau du premier état à un deuxième état qui appelle une première fonction de traitement du message, en passant comme paramètres de ladite première fonction, au moins une adresse de deuxième fonction et un pointeur sur la zone de la mémoire;
- 10 - un acquittement de la première fonction avant traitement du message, fait immédiatement repasser la couche de sécurité réseau dans l'état initial;
- un branchement sur l'adresse de deuxième fonction après traitement du message, fait passer la couche de sécurité réseau de l'état initial à un troisième état qui réalise une restitution du contexte d'exécution avant de faire repasser la couche de sécurité réseau dans l'état initial.
- 15

Dans l'état initial, la couche de sécurité réseau n'utilise aucune ressource du dispositif informatique. Le retour de la couche de sécurité réseau dans son état initial sans attendre une fin de traitement du message évite de bloquer le dispositif informatique. La sauvegarde du contexte d'exécution permet de replacer en fin de traitement de message, la couche de sécurité réseau dans le contexte où elle était avant que le traitement commence. Ainsi, le traitement de sécurisation du message est effectué de façon asynchrone.

20

25

Une description de mise en œuvre particulière de l'invention, suit en référence aux figures où:

- la figure 1 représente une architecture de réseau sécurisé;
- 30 - la figure 2 représente un dispositif informatique pour traiter des messages;
- la figure 3 représente les étapes essentielles d'une couche de traitement de sécurité sous forme de machine à nombre fini d'états de l'état de la technique;
- les figures 4 et 5 représentent les étapes essentielles d'une couche de traitement de sécurité sous forme de machine à nombre fini d'états conforme à l'invention;

- la figure 6 représente les étapes essentielles d'un pilote de carte de traitement matériel sous forme de machine à nombre fini d'états pour mettre en œuvre la machine selon les figures 3 et 4.
- la figure 7 représente une architecture de zones de sauvegardes en mémoire;
- 5 - la figure 8 présente une première étape d'un procédé de réalisation de code d'une couche de sécurité réseau;
- la figure 9 présente une deuxième étape du procédé de réalisation de code d'une couche de sécurité réseau;
- la figure 10 présente un procédé de production de messages sécurisés.

10

En référence à la figure 1, un dispositif informatique 67 est physiquement relié à un premier réseau privé 69 et un dispositif informatique 68 est physiquement relié à un deuxième réseau privé 70. Des messages peuvent circuler en toute confidentialité sur chacun des réseaux privés 69 et 70 dans la mesure où aucune intrusion ne peut être effectuée de l'extérieur sur ces réseaux. Cependant, si le dispositif 67 envoie un message au dispositif 68 en utilisant des services d'un réseau public 71, la confidentialité n'est pas assurée sans prendre de précautions particulières. Le réseau public 71 est par exemple le réseau connu sous le nom d'Internet, souvent représenté sous forme d'un nuage dans la littérature. Le réseau public 71 regroupe plusieurs réseaux 72, 73, interconnectés au moyens de dispositifs informatiques tels qu'un dispositif informatique 65 non contrôlé par les dispositifs 67, 68.

15

20

Le réseau privé 69 est relié au réseau public 71 par un dispositif informatique 66 et le réseau privé 70 est relié au réseau public 71 par un dispositif informatique 1. Les dispositifs informatiques 1 et 66 sont appelés passerelles dans la suite de la description. Chaque dispositif informatique 1, 65, 66, 67, 68 comprend traditionnellement une couche réseau utilisant un protocole de communication tel que le protocole connu IP, surmonté d'une couche transport utilisant un protocole tel que le protocole connu TCP, UDP ou autre, surmonté à son tour d'une couche applicative telle que http, ftp ou autre qui émettent et reçoivent des messages. Si un message traverse les couches TCP puis IP dans le dispositif 67 et traverse les couches IP puis TCP dans le dispositif 68, l'acheminement du message à travers le réseau public 71 reste normalement dans les couches IP des dispositifs 66, 65, 1.

25

30

Cependant, le dispositif 65 peut favoriser une intrusion étrangère sur les réseaux 72, 73 avec un danger de capter le message pour le lire, le modifier, voire de générer un message en se faisant passer pour le dispositif 67. Une solution consiste à crypter et/ou signer le message dans la couche IP de la passerelle 66, à sa sortie sur le réseau d'interconnexion 72, puis de décrypter le message dans la couche IP de la passerelle 1, à son entrée du réseau d'interconnexion 73. Une solution connue sous le nom d'Ipsec, permet ainsi de créer un tunnel 74 qui traverse le réseau public 71, de façon à créer un réseau privé virtuel utilisables par les dispositifs 67 et 68.

- 10 En référence à la figure 2, un dispositif informatique 1 comprend une mémoire 2, une ou plusieurs cartes d'accès réseau 3 et une ou plusieurs cartes de cryptographie 4. La carte d'accès réseau 3 est destinée à être raccordée sur une ou plusieurs liaisons physiques, non représentées. La mémoire 2, de type connu tel que les mémoires à accès aléatoire RAM, est destinée à contenir des données et des programmes de traitement du dispositif
- 15 informatique 1. La carte d'accès réseau 3 est de type connu telle que par exemple ethernet, pour recevoir et émettre des messages circulant sur un réseau informatique. La carte de cryptographie 4 est destinée à coder et décoder des messages sécurisés au moyen de circuits matériels dédiés qui mettent en œuvre des algorithmes de cryptage de type connus tels que par exemple tripleDES. Les circuits matériels dédiés, non
- 20 représentés, permettent un traitement de codage et décodage plus rapide que des programmes purement logiciels. Ces circuits ne font pas l'objet de la présente invention.

La mémoire 1 comprend des données et des programmes d'une couche utilisateur 5 et d'une couche noyau 6. La couche utilisateur 5 est de type connu pour exécuter des applications telles que des applications clientes ou serveur sur Internet comme http, www, telnet ou autres. La couche noyau 6 est destinée à contenir des structures de données et des fonctions primitives d'un système d'exploitation tel que par exemple le système d'exploitation connu LINUX.

- 30 La couche noyau 6 comprend une couche réseau 7 et un pilote 8. La couche réseau 7 est destinée à exécuter des protocoles réseaux tels que par exemple le protocole IP. La couche réseau 7 comprend une couche sécurité 9 destinée à exécuter des protocoles de communication sécurisée tels que par exemple Ipsec. Le pilote 8 est destiné à

commander la carte de cryptographie 4, essentiellement sur demande de la couche sécurité 9.

En référence à la figure 3, dans un état initial 12, la couche sécurité réseau 9 ne consomme aucune ressource du système. Sur détection d'un message à sécuriser, une transition 13, 14, 15, 16 fait passer la couche sécurité réseau respectivement dans un état 17, 18, 19, 20 qui appelle une fonction F1, F2, F3, F4 de traitement du message. Au retour de la fonction appelée F1, F2, F3, F4, une transition 21, 22, 23, 24, signalant que le message est traité, fait repasser la couche sécurité réseau 9 dans l'état initial 12, libérant ainsi les ressources systèmes nécessaires à la couche sécurité réseau 9.

La transition 13 correspond à une détection de message M1 à décrypter. La fonction F1 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de décrypter le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires au décryptage du message. Par exemple, dans le cas de l'algorithme tripleDES, la carte de cryptographie dispose de la clef secrète pour décoder le message. Lorsque la carte de cryptographie 4 a terminé de décrypter le message, le pilote 8 valide la transition 21 en remettant le message M1 à disposition de la couche sécurité réseau 9.

La transition 14 correspond à une détection de message M2 à authentifier. La fonction F2 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 d'authentifier le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires à l'authentification du message. Par exemple, dans le cas de l'algorithme HMAC-SHA1, la carte de cryptographie dispose de la clef secrète de façon à vérifier la signature de la passerelle 66. Lorsque la carte de cryptographie 4 a terminé d'authentifier le message, le pilote 8 valide la transition 22 en remettant le message M2 à disposition de la couche sécurité réseau 9.

La transition 15 correspond à une détection de message M4 à signer. La fonction F4 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de signer le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires pour signer le message. Par exemple, dans le cas de l'algorithme HMAC-SHA1, la carte de cryptographie dispose de la clef secrète pour élaborer sa signature.

Lorsque la carte de cryptographie 4 a terminé de signer le message, le pilote 8 valide la transition 21 en remettant le message M4 à disposition de la couche sécurité réseau 9.

La transition 16 correspond à une détection de message M3 à crypter. La fonction F3
 5 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de crypter le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires au cryptage du message. Par exemple, dans le cas de l'algorithme tripleDES, la carte de cryptographie dispose de la clef secrète pour coder le message. Lorsque la carte de cryptographie 4 a terminé de crypter le message, le pilote 8 valide la
 10 transition 24 en remettant le message M3 à disposition de la couche sécurité réseau 9.

L'inconvénient de l'état de la technique ici décrit en référence à la figure 3 est que le traitement du message nécessite d'être terminé pour permettre à la couche sécurité réseau 9 de revenir à l'état initial 12 et libérer les ressources du système ou être
 15 disponible pour un traitement ultérieur d'un autre ou du même message. En effet un message qui se présente par exemple comme message M1 à décrypter peut se présenter comme message M2 à authentifier après avoir été décrypté. Toutes les combinaisons sont possibles. Or les traitements de cryptage et de décryptage sont particulièrement longs, même effectués au moyen de circuits matériels.

20

En référence à la figure 4, dans un état initial 12, la couche sécurité réseau 9 ne consomme aucune ressource du système. Sur détection d'un message M1, M2, M4, M3, auquel appliquer un traitement de sécurité, une transition 13, 14, 15, 16 fait passer la couche sécurité réseau respectivement dans un état 25, 26, 27, 28 qui déclenche une
 25 séquence de sauvegarde F5, F6, F7, F8 du contexte d'exécution en cours CE. En fin de séquence F5, F6, F7, F8, une transition 29, 30, 31, 32, est validée par une valeur de pointeur PZS(M1), PZS(M2), PZS(M4), PZS(M3) sur une zone de sauvegarde résultant de l'état précédent 25, 26, 27, 28.

30 Les traitements de sécurité, décryptage en aval de la transition 13, authentification en aval de la transition 14, signature en aval de la transition 15, cryptage en aval de la transition 16, sont considérés à titre d'exemple non limitatif en référence aux figures 3 et 4, comparativement à la figure 3. L'enseignement de l'invention reste valable pour tout autre traitement tel que résumé (digest en anglais) ou compression de message.

Chaque séquence de sauvegarde F5, F6, F7, F8 est spécifique du traitement à effectuer pour chaque type de message M1, M2, M4, M3. La séquence F5, F6, F7, F8 consiste essentiellement à sauvegarder dans une zone mémoire le contexte d'exécution CE en cours. Le contexte d'exécution CE en cours est constitué de variables locales et globales qui sont utilisées par la couche sécurité réseau 9 pour le traitement du message telles que caractéristiques de sécurité du message, protocoles et clefs à employer. Le début de la zone mémoire est repérée par un pointeur PZS(M1), PZS(M2), PZS(M4), PZS(M3) de façon à ce que le contexte d'exécution CE lié au traitement du message M1, M2, M4, M3, puisse être restitué ultérieurement.

Lorsque la séquence F5 a terminé de sauvegarder le contexte d'exécution CE, la transition 29 fait passer la couche sécurité réseau 9 dans un état 33 qui effectue un appel à une fonction F9 exécutée par le pilote 8 pour commander à la carte 4, un décryptage du message M1. La fonction F9 passe en paramètres, une adresse @F13 de fonction dite de retour, une variable dite de corrélation VC1 et la valeur du pointeur PZS(M1).

Une transition 37 est validée par un acquittement de la fonction F9, retourné par le pilote 8. La transition 37 refait passer la couche sécurité réseau 9 dans son état initial 12.

Lorsque la séquence F6 a terminé de sauvegarder le contexte d'exécution CE, la transition 30 fait passer la couche sécurité réseau 9 dans un état 34 qui effectue un appel à une fonction F10 exécutée par le pilote 8 pour commander à la carte 4, une authentification du message M2. La fonction F10 passe en paramètres, une adresse @F14 de fonction dite de retour, une variable dite de corrélation VC2 et la valeur du pointeur PZS(M2).

Une transition 38 est validée par un acquittement de la fonction F10, retourné par le pilote 8. La transition 38 refait passer la couche sécurité réseau 9 dans son état initial 12.

Lorsque la séquence F7 a terminé de sauvegarder le contexte d'exécution CE, la transition 31 fait passer la couche sécurité réseau 9 dans un état 35 qui effectue un

appel à une fonction F11 exécutée par le pilote 8 pour commander à la carte 4, une signature du message M4. La fonction F11 passe en paramètres, une adresse @F15 de fonction dite de retour, une variable dite de corrélation VC4 et la valeur du pointeur PZS(M4).

5

Une transition 39 est validée par un acquittement de la fonction F11, retourné par le pilote 8. La transition 39 refait passer la couche sécurité réseau 9 dans son état initial 12.

10

Lorsque la séquence F8 a terminé de sauvegarder le contexte d'exécution CE, la transition 32 fait passer la couche sécurité réseau 9 dans un état 36 qui effectue un appel à une fonction F12 exécutée par le pilote 8 pour commander à la carte 4, une signature du message M3. La fonction F12 passe en paramètres, une adresse @F16 de fonction dite de retour, une variable dite de corrélation VC3 et la valeur du pointeur

15

PZS(M3).

Une transition 40 est validée par un acquittement de la fonction F12, retourné par le pilote 8. La transition 40 refait passer la couche sécurité réseau 9 dans son état initial 12.

20

La figure 6 présente des états et transition du pilote 8 de carte de cryptographie particulièrement adaptés pour s'interfacer avec les états et transitions de la couche sécurité réseau 9 conforme à l'invention, en référence aux figures 3 et 4. D'autres états du pilote, applicables à la commande de la carte 4, ne sont pas décrits ici car ces autres états sortent du cadre de la présente invention. Les états décrits sont ceux qui correspondent aux traitement de cryptage et de décryptage. L'enseignement qui en résulte est applicable à l'authentification, la signature et ou à tout autre traitement de sécurisation tel que le résumé de message au moyen de la carte matérielle 4.

25

30

Dans un état initial 41, le pilote 8 n'utilise aucune ressource du système. Une transition 42 est activée par l'appel de la fonction F9, effectué dans l'état 33 de la couche sécurité réseau 9. Une transition 43 est activée par l'appel de la fonction F12, effectué dans l'état 36 de la couche sécurité réseau 9.

La transition 42 fait passer le pilote 8 dans un état 44. Dans l'état 44, le pilote 8 envoie immédiatement acquittement Acq(F9) qui valide la transition 37 et active la carte 4 pour effectuer un traitement matériel de décryptage du message M1. La carte 4 prend alors en charge le message M1. Dès que la carte 4 est activée, une transition 46 refait passer le pilote dans l'état initial 41 qui le rend disponible pour prendre en charge d'autres demandes de traitement par la couche de sécurité réseau 9.

Lorsque la carte 4 a terminé de décrypter le message M1, une transition 48 fait passer le pilote dans un état 50. Dans l'état 50, le pilote effectue un branchement sur l'adresse @F13 de fonction de retour en communiquant le pointeur PZS(M1) précédemment donnés dans l'état 33 de la couche de sécurité réseau. Le pilote place également dans la variable de corrélation VC1, les coordonnées de mise à disposition du message M1 décrypté par la carte 4. Puis le pilote retourne dans son état initial 41.

La transition 43 fait passer le pilote 8 dans un état 45. Dans l'état 45, le pilote 8 envoie immédiatement acquittement Acq(F12) qui valide la transition 40 et active la carte 4 pour effectuer un traitement matériel de cryptage du message M3. La carte 4 prend alors en charge le message M3. Dès que la carte 4 est activée, une transition 47 refait passer le pilote dans l'état initial 41 qui le rend disponible pour prendre en charge d'autres demandes de traitement par la couche de sécurité réseau 9.

Lorsque la carte 4 a terminé de crypter le message M3, une transition 49 fait passer le pilote dans un état 51. Dans l'état 51, le pilote effectue un branchement sur l'adresse @F16 de fonction de retour en communiquant le pointeur PZS(M3) précédemment donnés dans l'état 36 de la couche de sécurité réseau. Le pilote place également dans la variable de corrélation VC3, les coordonnées de mise à disposition du message M3 crypté par la carte 4. Puis le pilote retourne dans son état initial 41.

En référence à la figure 5, une transition 52 fait passer la couche sécurité réseau de l'état initial 12 à un état 56, une transition 53 fait passer la couche sécurité réseau de l'état initial 12 à un état 57, une transition 54 fait passer la couche sécurité réseau de l'état initial 12 à un état 58, une transition 55 fait passer la couche sécurité réseau de l'état initial 12 à un état 59.

La transition 52 est validée par le branchement sur l'adresse @F13 et la communication du pointeur PZS(M1) effectués dans l'état 50. Dans l'état 56, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M1). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 25 pour le message M1 alors que le message M1 n'était pas décrypté. Cependant, le message étant à présent décrypté, la variable de corrélation VC1 valide immédiatement une transition 60 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC1 met le message M1 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau ou pour présenter le message M1 traité comme message de type M2, M3, M4 pour un autre traitement. Pour mettre le message M1 à disposition de la couche de sécurité réseau 9, la valeur de la variable de corrélation VC1 est par exemple une valeur permettant de reprendre l'exécution à un endroit adéquat.

La transition 55 est validée par le branchement sur l'adresse @F16 et la communication du pointeur PZS(M3) effectués dans l'état 51. Dans l'état 59, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M3). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 28 pour le message M3 alors que le message M3 n'était pas crypté. Cependant, le message étant à présent crypté, la variable de corrélation VC3 valide immédiatement une transition 64 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC3 met le message M3 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M3 traité comme message de type M2, M1, M4 pour un autre traitement.

De même, la transition 53 est validée par le branchement sur l'adresse @F14 et la communication du pointeur PZS(M2) effectués dans un état non représenté du pilote 8. Dans l'état 57, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M2). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 26 pour le message M2 alors que le message M2 n'était pas authentifié. Cependant, le message étant à présent authentifié, la variable de corrélation VC2 valide immédiatement une transition 62 qui replace la couche de sécurité réseau dans son état

initial 12. La variable de corrélation VC2 met le message M2 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M2 traité comme message de type M1, M3, M4 pour un autre traitement.

5

De même, la transition 54 est validée par le branchement sur l'adresse @F15 et la communication du pointeur PZS(M4) effectués dans un état non représenté du pilote 8. Dans l'état 58, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M4). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 27 pour le message M4 alors que le message M2 n'était pas signé. Cependant, le message étant à présent signé, la variable de corrélation VC4 valide immédiatement une transition 63 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC4 met le message M4 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M4 traité comme message de type M1, M3, M2 pour un autre traitement.

15

Prenons sur la figure 2 un cheminement 10 de message crypté M1 de la carte réseau 3 à la carte de cryptographie 4 suivi d'un cheminement 11 du message décrypté M1 de la carte 4 à la mémoire 2 pour sa présentation par exemple à la couche utilisateur 5.

20

Lorsque le message M1 en provenance de la carte 3 est transmis à la mémoire 2 selon la branche ascendante du cheminement 10, sa présentation à la couche de sécurité réseau 9 valide la transition 13. La couche de sécurité réseau 9 reste peu de temps dans l'état 25 car la sauvegarde du contexte d'exécution est une opération relativement rapide. A la suite de l'état 25, la couche de sécurité réseau 9 reste peu de temps dans l'état 33 car l'état 44 du pilote 8 envoie l'acquittement Acq(F9) immédiatement après l'appel de la fonction F9 sans attendre que le message M1 soit décrypté. La couche de sécurité réseau 9 retourne donc rapidement dans son état initial 12. D'une part, ceci évite au système de rester bloqué pendant le traitement de décryptage du message M1 car ce traitement est pris en charge par la carte 4 de façon asynchrone. D'autre part, ceci présente l'avantage de rendre la couche de sécurité réseau rapidement à nouveau disponible pour une présentation d'un autre message à traiter.

30

Lorsque le message M1 est rangé décrypté par la carte 4 en mémoire 2 selon une première branche ascendante du cheminement 11, l'état 50 du pilote 8 valide la transition 52 de la couche sécurité réseau 9. La couche de sécurité réseau 9 reste peu de temps dans l'état 56 qui en résulte, car la restitution du contexte d'exécution CE est
5 une opération relativement rapide. En fin de restitution de contexte CE, la transition 21 remplace rapidement la couche de sécurité réseau 9 dans l'état initial 12 car la valeur de corrélation VC1 met immédiatement le message M1 sous forme décryptée à disposition de la couche sécurité réseau 9 pour être retransmis; dans le cas de la figure 2, à la couche utilisateur 5 selon une deuxième branche ascendante du cheminement 11. Ainsi,
10 le temps de décryptage du message M1 est totalement transparent pour la couche de sécurité réseau 9, activée seulement un court instant après présentation du message M1 à décrypter, puis réactivée seulement un court instant après présentation du message M1 décrypté. Les cheminement 10 et 11 de la figure 2 sont symboliques dans le but uniquement de montrer l'intérêt de l'invention. L'homme du métier sait par ailleurs qu'une
15 ou plusieurs couches peuvent séparer la couche réseau 7 de la couche utilisateur 5, telle qu'une couche transport de type connu TCP, non représentée de façon à ne pas surcharger inutilement la figure 2. D'autre part, le cheminement 11 peut aussi être redirigé vers la carte 3 par la couche réseau 7 ou à nouveau vers la carte 4 pour un traitement subséquent.

20 Comme la couche noyau 6 n'est pas bloquée en attente de fin de traitement d'un message, il est intéressant de faire prendre en charge d'autres messages qui se présentent à la couche sécurité réseau 9 alors qu'un premier message n'est pas encore terminé d'être traité.

25 En référence à la figure 7, pendant que le message M1 est pris en charge par la carte 4 pour être décrypté, le pointeur PZS(M1) a pour valeur celle d'un mot 56 qui contient une adresse de début d'une zone 52 de la mémoire 2. La zone 52 contient le contexte d'exécution CE lorsque la couche sécurité réseau était dans l'état 25 pour le message
30 M1. Un mot 55 est destiné à contenir une adresse suivant une dernière adresse de la zone 52. Ainsi, le mot 55 définit un pointeur de zone libre PZL sur une zone de sauvegarde de contexte d'exécution suivante 53.

Lorsqu'un autre message M'1 se présente à la couche de sécurité réseau 7, la valeur du mot 55 est transférée dans un mot 57 pour définir un nouveau pointeur PZS(M'1) sur le début de la zone 53 où est sauvegardé le contexte d'exécution CE lorsque la couche sécurité réseau est dans l'état 25 pour le message M'1. Le mot 55 est contient alors une
 5 adresse suivant une dernière adresse de la zone 53. Ainsi, le mot 55 définit un pointeur de zone libre PZL sur une zone de sauvegarde de contexte d'exécution suivante 54, disponible pour le contexte d'exécution CE lié à un nouveau message M''1. Ce processus est répété pour tout nouveau message de façon à chaîner les sauvegardes de contexte d'exécution CE.

10

Suite à une restitution de contexte d'exécution CE dans l'état 56 de la couche de sécurité réseau, l'adresse de début de la zone de sauvegarde libérée est prise comme adresse suivante de la dernière zone de sauvegarde occupée selon un mécanisme de chaînage classique.

15

Il est possible d'utiliser une structure de données semblable à celle qui vient d'être décrite, distincte pour chacun des états 25, 26, 27, 28 de la couche de sécurité réseau, ou commune à tous les états 25, 26, 27, 28, auquel cas les mots 56, 57 peuvent contenir des PZS(M1), PZS(M2), PZS(M3), PZS(M4) pour l'un quelconque de ces états.

20

La couche de sécurité réseau peut être programmée de différentes manières pour mettre en œuvre les états précédemment décrits. Un procédé de réalisation de code de la couche de sécurité réseau 9 à partir d'une couche de sécurité réseau standard telle que par exemple la couche Ipsec de LINUX, comprend essentiellement deux étapes.

25

La première étape est expliquée en référence à la figure 8. Dans la couche noyau 6 du dispositif informatique 1, une première séquence de code 75 est destinée à être activée par une présentation de message M1, M2, M3 ou M4 auquel appliquer un traitement de sécurisation, décryptage, authentification, cryptage ou signature. Dans la couche de
 30 sécurité réseau standard, la séquence de code 75 est constituée de plusieurs lignes de code standard qui ne font pas l'objet de la présente invention. On distingue à ce stade uniquement une ligne 76 et une dernière ligne de la séquence 75 repérée par un indicateur de Fin. La ligne 76 contient un appel à la fonction de traitement de

sécurisation standard, par exemple la première fonction F1 si la séquence de code 75 est celle activée par la présentation du message M1.

La première séquence de code 75 est modifiée en insérant avant la ligne 75, une
 5 deuxième séquence de code 77. La séquence de code 77 commence par une ou
 plusieurs lignes F5(CE) qui sauvegardent le contexte d'exécution CE en cours lorsque la
 première séquence est activée, c'est à dire essentiellement les valeurs des variables
 locales et globales utilisées dans la séquence de code 75. Le code de sauvegarde
 10 consiste alors en des écritures des valeurs de ces variables dans une zone de la
 mémoire 2, repérée par le pointeur PZS(M1).

A la suite des lignes F5(CE), la séquence 77 contient le code d'appel à une deuxième
 fonction de sécurisation, par exemple la fonction F9(@F13, VC1, PZS(M1)) dans le cas
 ici décrit. La deuxième fonction est destinée à être exécutée par le pilote 8. Les
 15 paramètres passés sont essentiellement une adresse de fonction @F13 et le pointeur
 PZS sur la zone de sauvegarde.

La séquence de code 77 se termine par un branchement sur la dernière ligne de la
 séquence de code 75 de type "Goto Fin".

20

La deuxième étape est expliquée en référence à la figure 9. La première séquence de
 code 75 est copiée de façon à générer une troisième séquence de code 78, prise
 comme étant le code de la fonction F13 dont l'adresse @F13 est repérée par un pointeur
 81. Une quatrième séquence de code 80 est insérée après la ligne 76 de la séquence
 25 78. La séquence 80 est repérée par une étiquette et contient des instructions de lecture
 de la zone mémoire indiquée par le pointeur PZS. Une ligne 79 est insérée en début de
 séquence 78. La ligne 79 contient une instruction de branchement "Goto Etiquette" sur la
 séquence de code 80.

30 La couche de sécurité réseau (9) obtenue par le procédé précédemment décrit, est plus
 rapide que la couche de sécurité réseau standard d'origine. En effet, dans la couche de
 sécurité standard, l'exécution de la séquence 75 non modifiée s'effectue de la façon
 suivante. Les instructions de code standard qui précèdent la ligne 76 sont exécutées. La
 ligne 76 effectue un appel à la fonction de traitement standard F1. Les instructions de

code standard suivant la ligne 76 sont exécutées après le retour de la fonction F1 qui indique la fin de traitement du message. Or un traitement de cryptographie est long par nature. Ceci a pour effet de retarder l'atteinte en exécution de la dernière ligne "Fin" de la séquence 75 non modifiée.

5

Dans la couche de sécurité réseau obtenue par le procédé, l'exécution de la séquence 75 modifiée s'effectue de la façon suivante. Les instructions de code standard qui précèdent la ligne 76 et la séquence 77 sont exécutées. La ligne 76 et les lignes suivantes de la séquence 75 ne sont jamais exécutées à cause du premier branchement sur la dernière ligne de la séquence 75. Le premier branchement est effectué rapidement car la fonction F9 envoie immédiatement un acquittement avant que le message ne soit terminé d'être traité. Lorsque le traitement du message est terminé, le pilote 8 déclenche une exécution de la séquence de code 78 au moyen de l'adresse @F13. La ligne de code 76 et les lignes de code de la séquence 78 qui précèdent ne sont jamais exécutées à cause du branchement en début de séquence 78 sur la séquence 80 qui permet l'exécution des lignes de code suivantes, masquant ainsi le temps de traitement du message.

10

15

Le dispositif informatique qui vient d'être décrit permet de mettre en œuvre un procédé d'obtention d'un message sécurisé à partir d'un autre message.

20

En référence à la figure 10, sur présentation dudit autre message à la couche de sécurité réseau, dans une première étape 82, le contexte d'exécution en cours est sauvegardé. Cette étape est réalisée dans l'un des états 25, 26, 27, 28 de la couche 9.

25

Dans une deuxième étape 83, une requête de traitement de sécurisation est émise depuis la couche 9, dans l'un des états 33, 34, 35, 36, vers un élément extérieur à la couche 9, de façon à ce que la couche 9 soit remise dans son état initial qui n'utilise aucune ressource du dispositif. Les étapes 82 et 83 sont mises en œuvre au moyen de la séquence 77. Après que l'élément extérieur ait traité ledit autre message, le contexte sauvegardé est restitué dans une étape 84 de façon à produire le message sécurisé.

30

Ce procédé présente l'avantage de pouvoir produire des messages sécurisés en grand nombre car l'étape 84 peut être activée après plusieurs activations successives des étapes 82, 83 pour différents messages.

REVENDICATIONS:

1. Dispositif informatique (1) comprenant une mémoire (2) et une couche de sécurité réseau (9) pour appliquer un traitement de sécurisation sur présentation d'un message (M1) dans la mémoire (2), caractérisé en ce que:

- la présentation du message (M1) fait passer la couche de sécurité réseau (9) d'un état initial (12) à un premier état (25) qui réalise une sauvegarde de contexte d'exécution (CE) dans une zone (52) de la mémoire (2);

- la réalisation de la sauvegarde du contexte d'exécution (CE), fait passer la couche de sécurité réseau du premier état (25) à un deuxième état (33) qui appelle une première fonction (F9) de traitement du message (M1), en passant comme paramètres de ladite première fonction (F9), au moins une adresse (@F13) de deuxième fonction (F13) et un pointeur PZS(M1) sur la zone (52) de la mémoire (2);

- un acquittement de la première fonction (F9) avant traitement du message (M1), fait immédiatement repasser la couche de sécurité réseau dans l'état initial (12);

- un branchement sur l'adresse (@F13) de deuxième fonction, fait passer la couche de sécurité réseau (9) de l'état initial (12) à un troisième état (56) qui réalise une restitution du contexte d'exécution (CE) avant de faire repasser la couche de sécurité réseau (9) dans l'état initial.

2. Dispositif informatique (1) selon la revendication 1, caractérisé en ce que plusieurs pointeurs PZS(M1), PZS(M'1) sont chaînés de façon à pouvoir être restitués lors du branchement sur ladite adresse (@F13).

3. Dispositif informatique (1) selon la revendication 1 ou 2, caractérisé en ce que l'appel de la première fonction (F9) fait passer comme paramètre une variable de corrélation (VC1), restituée lors du branchement sur l'adresse (@F13).

4. Procédé de réalisation de code d'une couche rapide de sécurité réseau (9) à partir de code d'une couche standard de sécurité réseau dans une couche noyau (6) d'un dispositif informatique (1), caractérisé en ce qu'il comprend:

- une première étape pour modifier dans le code de ladite couche standard, une première séquence de code destinée à être activée par une présentation de message auquel appliquer un traitement de sécurisation, en insérant dans la première séquence,

avant un appel à une première fonction de sécurisation (F1), une deuxième séquence de code qui:

- commence par une sauvegarde d'un contexte d'exécution (CE) en cours lorsque la première séquence est exécutée,
- 5 - fait un appel à une deuxième fonction de sécurisation (F9),
- termine par un premier branchement sur la fin de la première séquence de code;
- une deuxième étape pour générer une troisième séquence de code d'une troisième fonction (F13) en copiant ladite première séquence de code modifiée puis en insérant
- 10 dans ladite troisième séquence de code:
 - après l'appel à la première fonction (F1), une quatrième séquence de code de restitution du contexte d'exécution (CE) sauvegardé,
 - en début de troisième séquence, un deuxième branchement sur ladite quatrième séquence de code.

15

5. Procédé pour obtenir un message sécurisé à partir d'un autre message, au moyen d'un dispositif informatique (1) comprenant une couche de sécurité réseau (9) à laquelle est présenté ledit autre message, caractérisé en ce qu'il comprend:

- une première étape pour sauvegarder un contexte d'exécution de la couche de sécurité
- 20 réseau après présentation du dit autre message;
- une deuxième étape dans laquelle la couche de sécurité réseau émet une requête de traitement de sécurisation vers un élément extérieur à la couche de sécurité réseau telle que ledit élément extérieur acquitte immédiatement cette requête de façon à mettre la couche de sécurité réseau dans un état initial qui n'utilise aucune ressource du dispositif
- 25 informatique (1);
- une troisième étape dans laquelle ledit élément extérieur active une restitution du contexte d'exécution sauvegardé dans la couche de sécurité réseau en présentant le message sécurisé par le traitement de sécurisation qui résulte de ladite requête.

Fig. 1

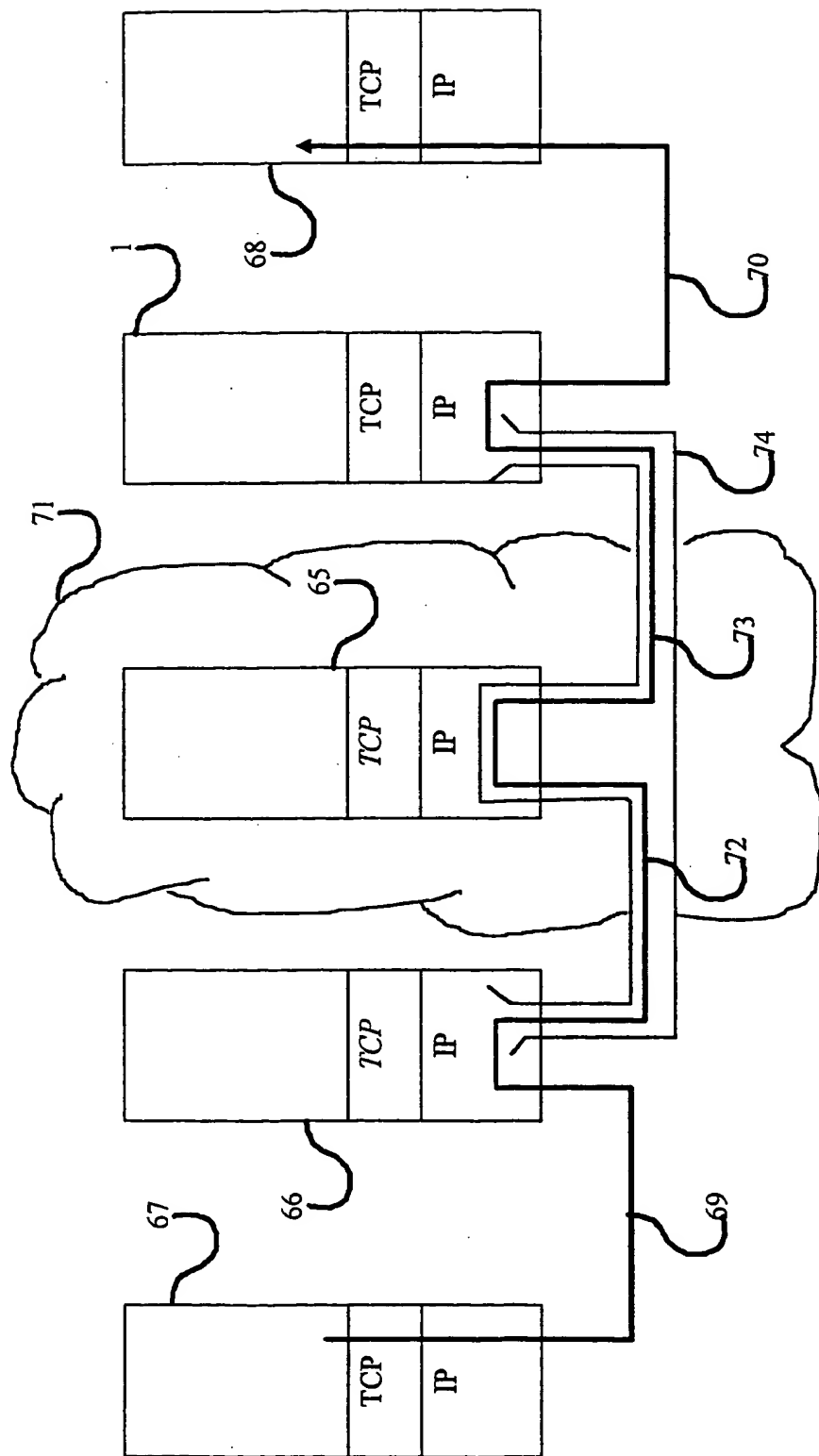


Fig.2

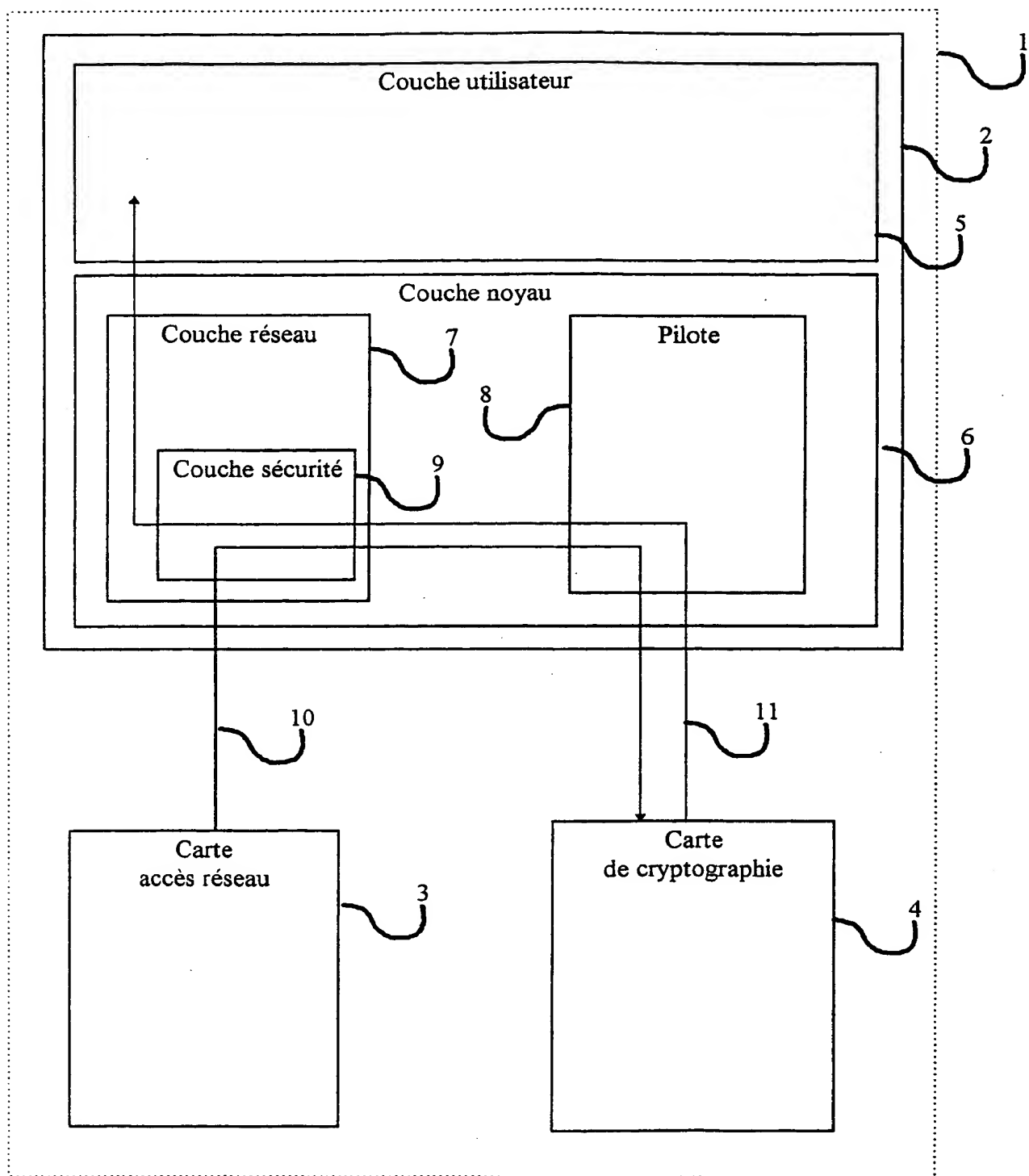


Fig.3

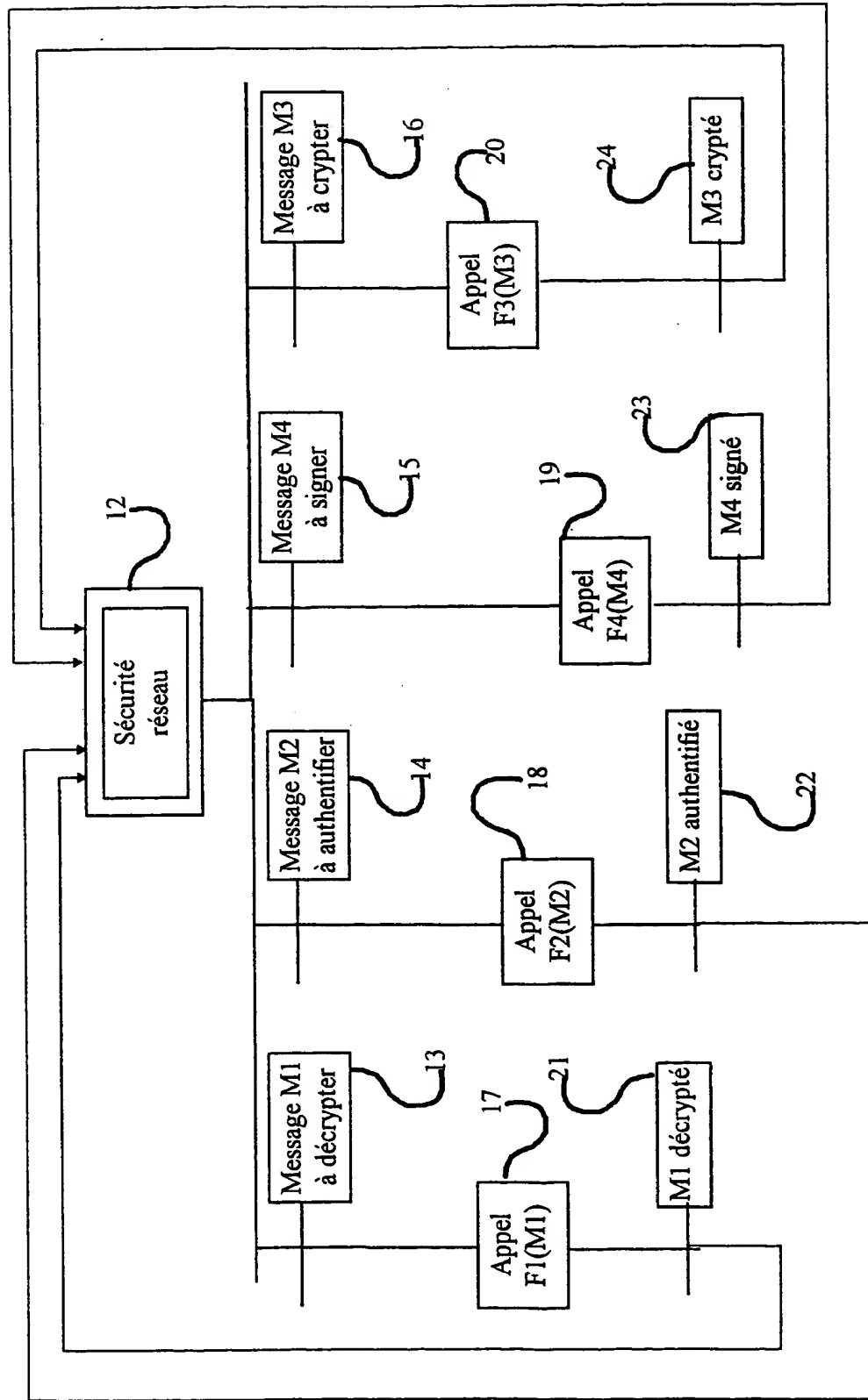


Fig. 4

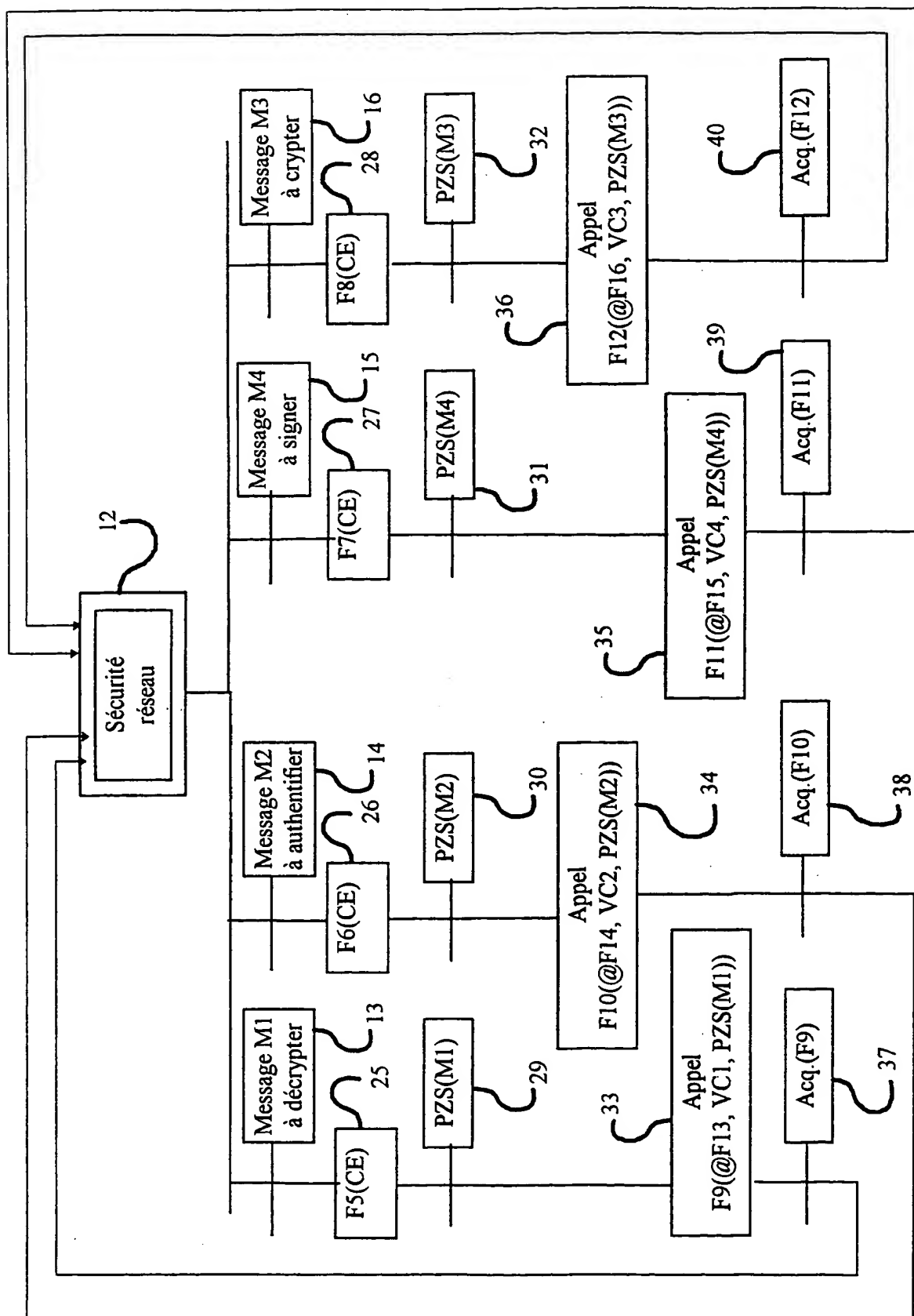


Fig. 5

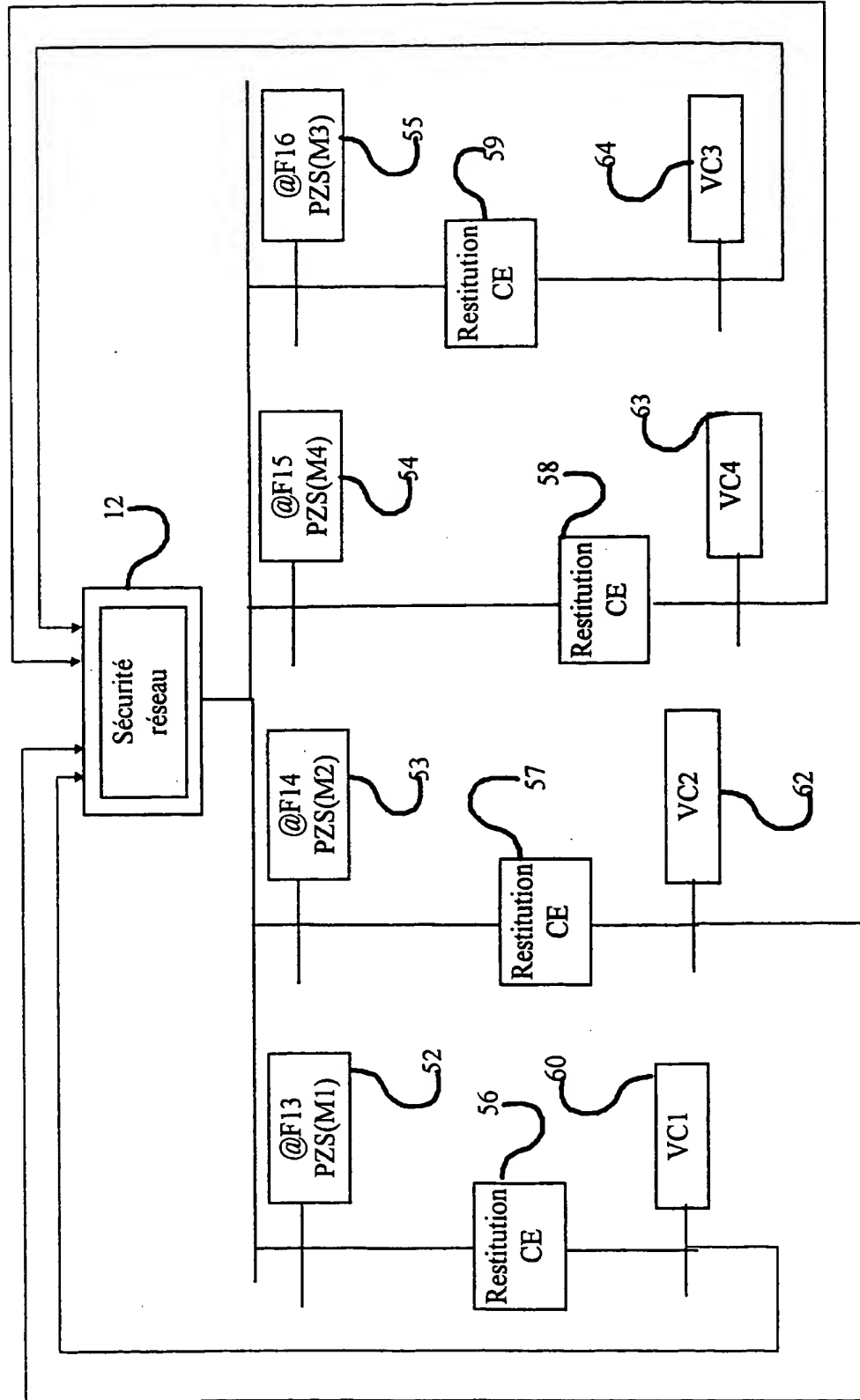


Fig. 6

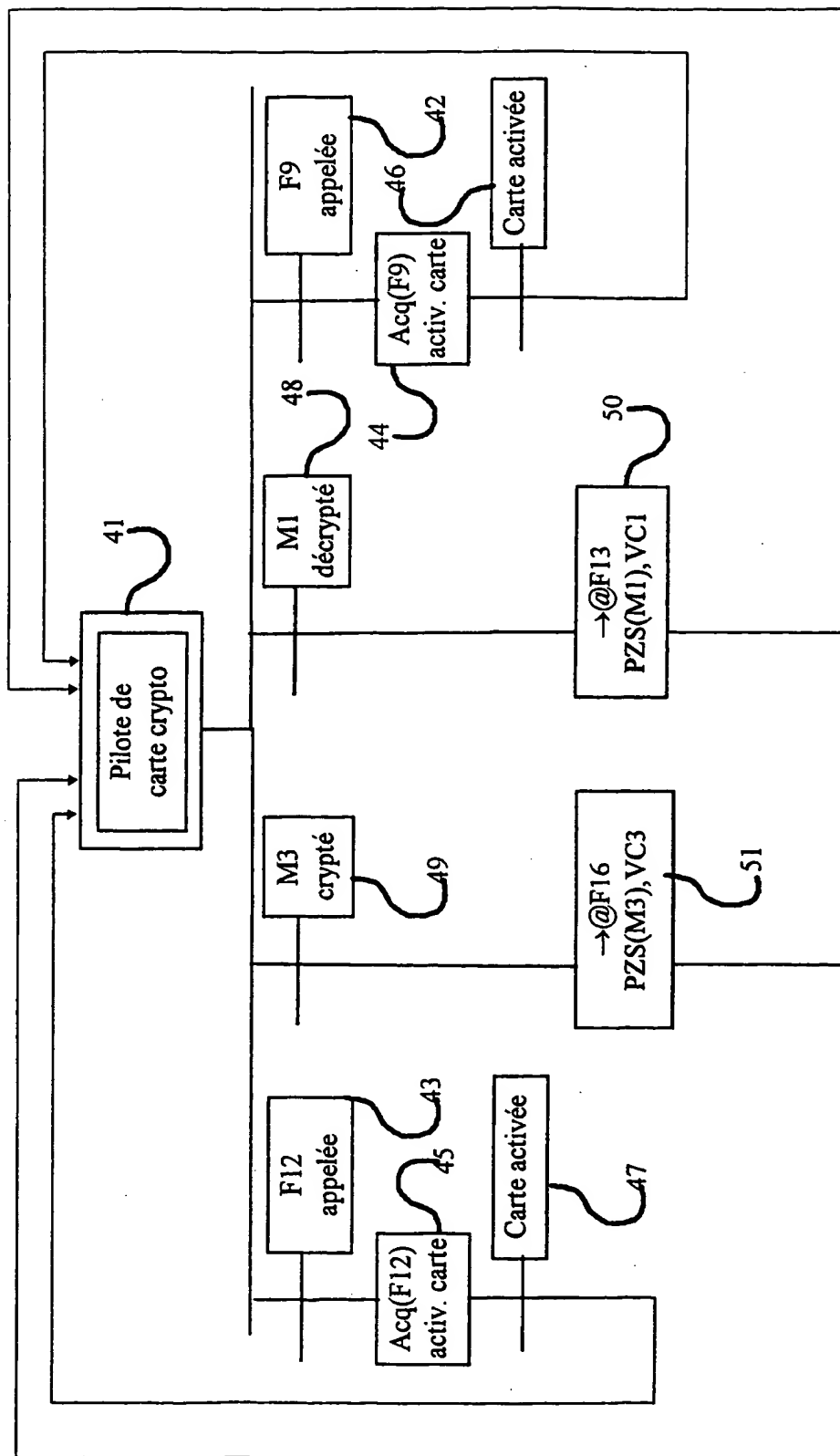


Fig. 7

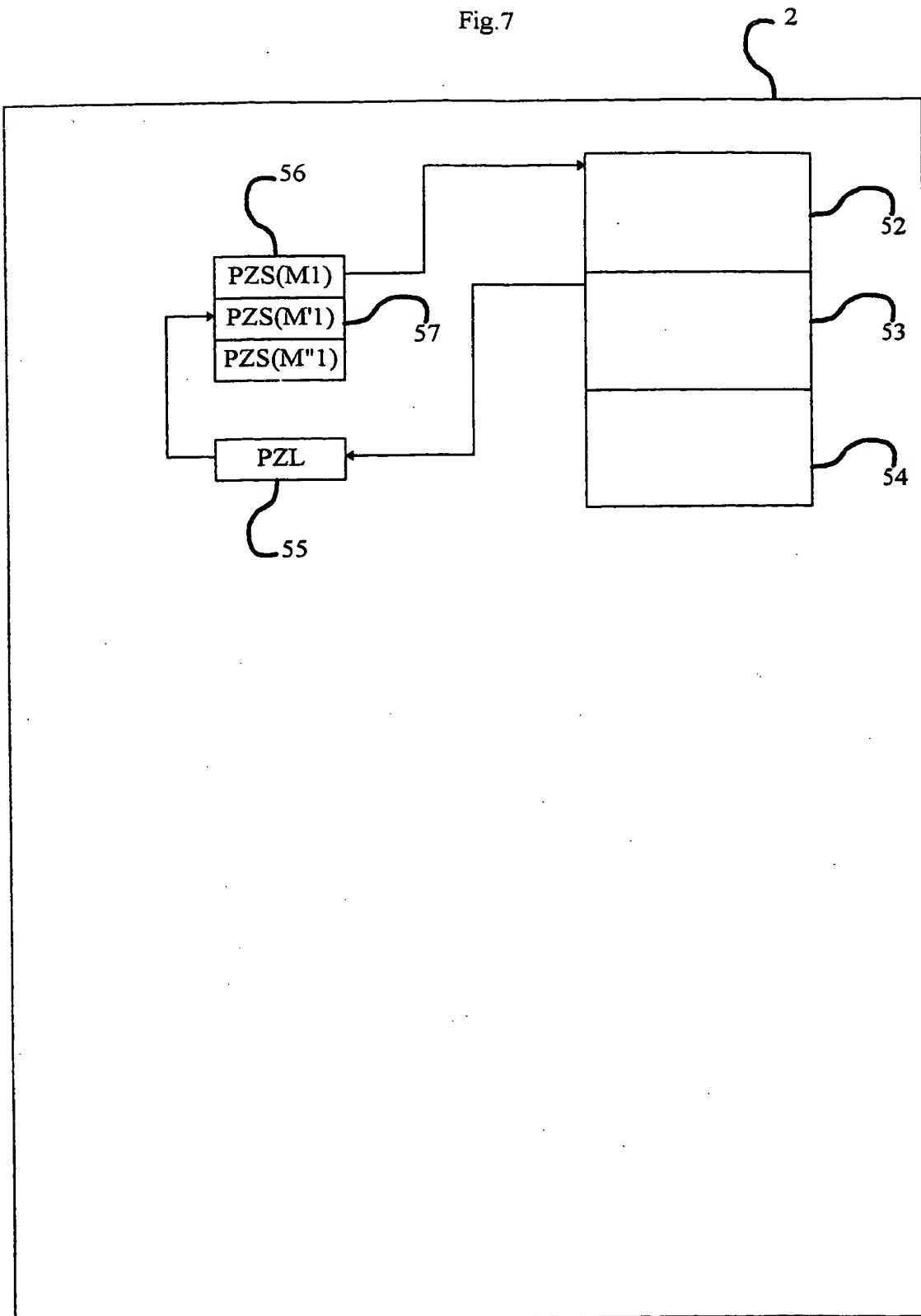


Fig.8

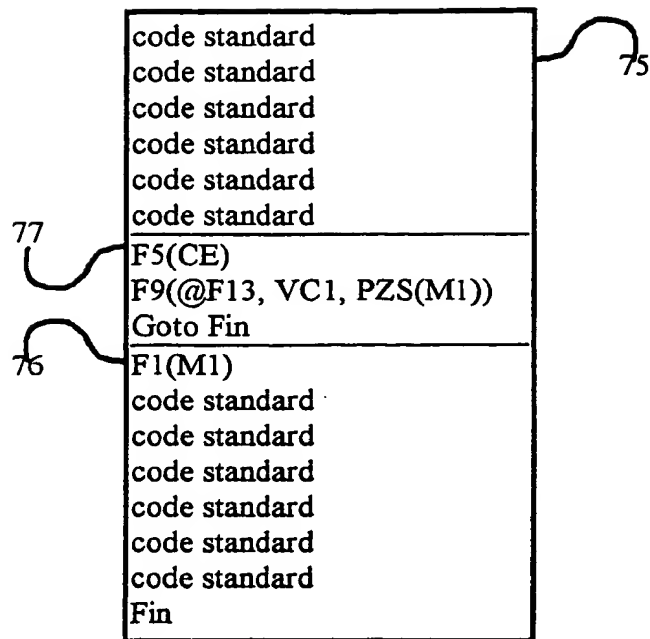


Fig.9

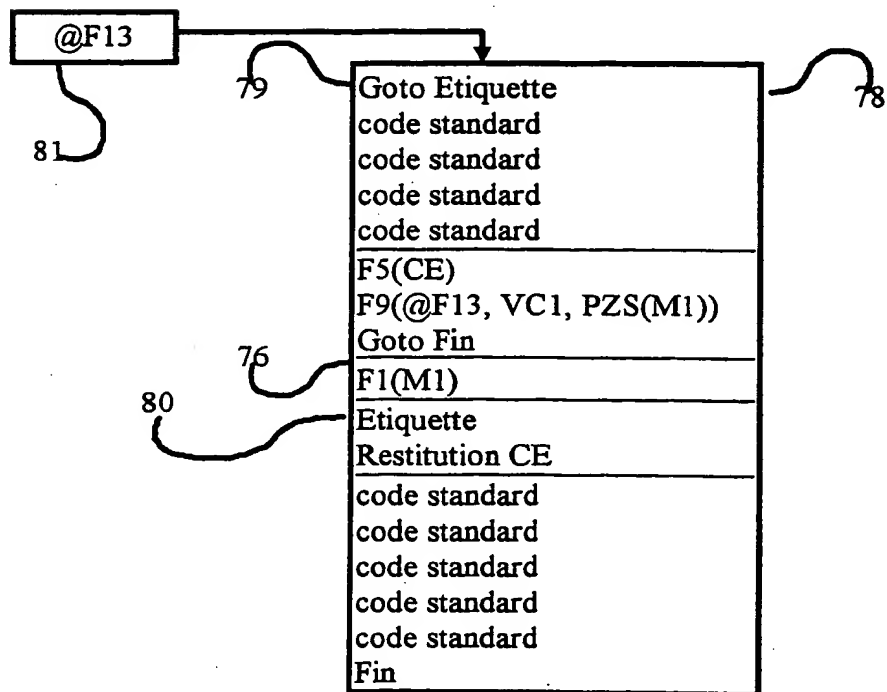


Fig. 10

